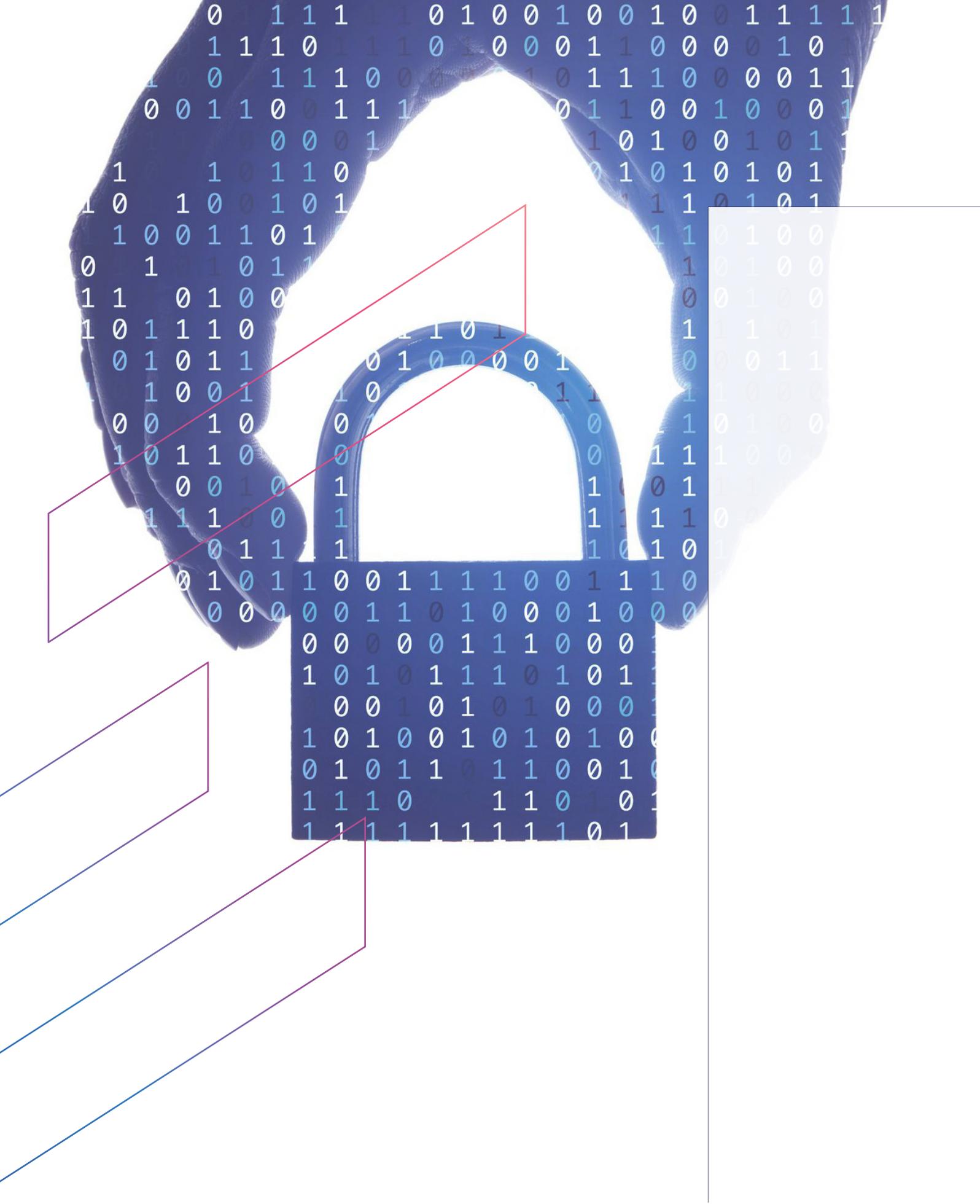




tessi

**L'OBSERVATOIRE TESSI
DE LA FRAUDE DOCUMENTAIRE**
RAPPORT INITIAL 2025



Executive Summary

LA FRAUDE DOCUMENTAIRE : UNE MENACE SYSTÉMIQUE POUR L'ÉCONOMIE FRANÇAISE

La fraude documentaire représente aujourd'hui une menace majeure pour l'économie française, avec des pertes annuelles estimées à **plus de 65 milliards d'euros, soit 2,5% du PIB national**. Notre étude révèle que ce phénomène s'intensifie, avec une augmentation de 244%¹ des fraudes numériques entre 2023 et 2024. Cette croissance alarmante s'explique en grande partie par la démocratisation des technologies numériques et l'émergence de l'IA générative. **10,8% des Français admettent avoir utilisé des faux documents, avec un taux de réussite inquiétant de 73%**.

65 milliards d'euros,
soit 2,5% du PIB national

Estimation de la fraude
documentaire en France

Aucun secteur n'est épargné par la fraude documentaire. Le secteur bancaire enregistre près de 1 milliard d'euros de pertes annuelles. **L'assurance, quant à elle, subit 2,5 milliards d'euros² de préjudice chaque année. Dans le domaine de la santé, les pertes pourraient atteindre 2,4 milliards d'ici 2027³.** Plus alarmant encore, la part de la fraude documentaire dans la fraude fiscale est estimée à 60 milliards d'euros.

Cette réalité est d'autant plus préoccupante que **69% des entreprises françaises ont été ciblées par au moins une tentative de fraude documentaire en 2022, ce taux atteignant 91% pour les grandes entreprises.**

Les études menées par Tessi confirment cette tendance. Celle sur « *Les Français et leur banque en 2024* », réalisée par IN BANQUE en partenariat avec Capgemini Invent et Tessi, révèle que **17% des Français connectés ont déjà falsifié des documents pour faciliter l'ouverture d'un compte ou l'obtention d'un crédit, un pourcentage qui dépasse 20% chez les moins de 35 ans.** De même, l'étude « *Innovation Assurance* » (2025) menée par Next Content en partenariat avec Tessi et Vector8 (février 2025) indique que **20% des assurés français ont déjà falsifié au moins un document parmi ceux couramment demandés par les assureurs.**

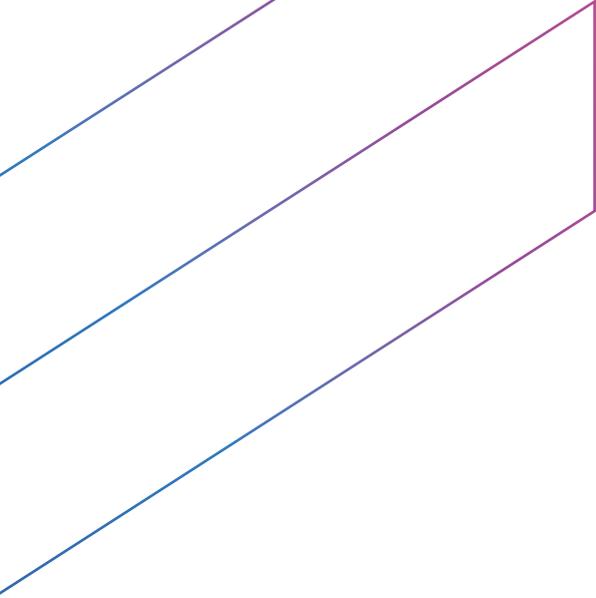
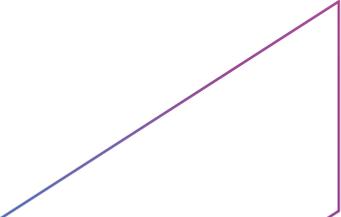
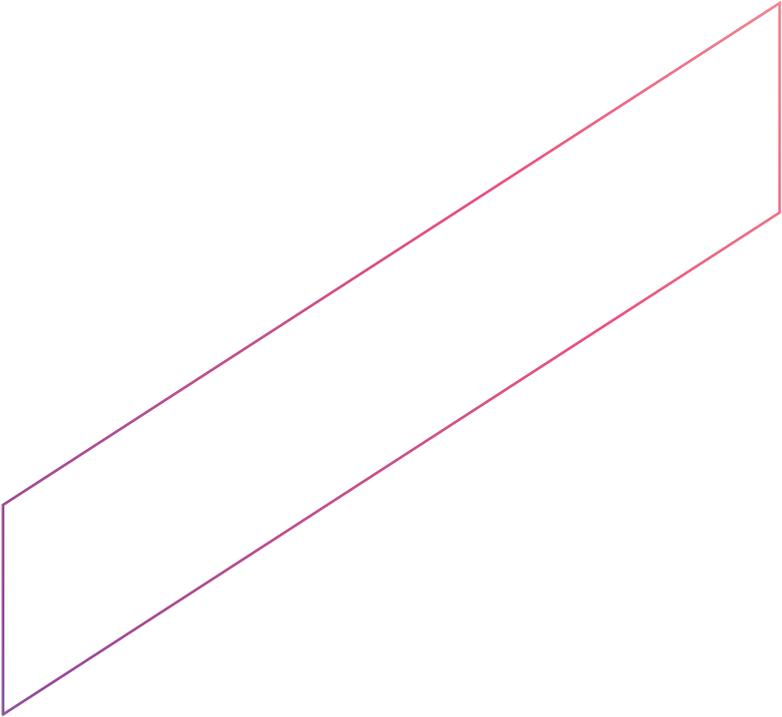
Face à ce défi, des solutions technologiques émergent, combinant Intelligence Artificielle (IA), biométrie, blockchain et vérification à la source. L'authentification biométrique, la vérification automatisée des documents et le futur portefeuille d'identité numérique européen (EUDI Wallet) constituent des avancées prometteuses. Cependant, ces approches techniques ne seront pleinement efficaces qu'accompagnées d'un renforcement des cadres réglementaires et d'une coopération accrue entre les acteurs publics et privés.

L'observatoire Tessi de la fraude documentaire s'engage à fournir une expertise pointue et des solutions adaptées pour lutter contre cette menace croissante. **Nous recommandons une approche globale associant digitalisation des contrôles, formation continue des équipes, adoption de politiques internes rigoureuses et sensibilisation de l'ensemble des parties prenantes.** La lutte contre la fraude documentaire n'est plus une option, mais une nécessité vitale pour la pérennité de notre économie.

1. Identity Fraud Report, 2025

2. Lutte contre la Fraude à l'Assurance (ALFA)

3. Assurance maladie, 2023



**L'OBSERVATOIRE TESSI
DE LA FRAUDE DOCUMENTAIRE
RAPPORT INITIAL 2025**



TABLE DES MATIÈRES

Introduction	6
Première partie	7
LA FRAUDE DOCUMENTAIRE : UNE MENACE SOUS ESTIMÉE AUX CONSÉQUENCES MAJEURES	
1.1 Comprendre les mécanismes de la fraude documentaire	7
1.2. Un impact économique massif et sous évalué	9
1.3. Pourquoi la fraude prospère : motivations et facteurs aggravants	12
1.4. Une menace sans frontières	13
Deuxième Partie	4
ANTICIPER ET CONTRER LA FRAUDE	
2.1 Que dit la loi	4
2.2. Une évolution du cadre légal qui s'impose	15
2.3. Comment les entreprises peuvent mieux se protéger	15
2.4. Les solutions technologiques pour lutter contre la fraude documentaire	16
2.5 L'importance de la sensibilisation et de la coopération intersectorielle	19
Conclusion	20
Glossaire de la Fraude Documentaire	21
Annexes	22

Introduction

La fraude documentaire représente aujourd'hui un enjeu majeur pour les particuliers, les entreprises, les administrations et l'économie nationale. Elle désigne la création et/ou l'utilisation de **documents falsifiés ou frauduleux dans le but d'obtenir des avantages illégitimes ou de commettre des activités criminelles**. Selon *La Revue Banque*, elle constitue la troisième plus grande industrie criminelle au monde derrière le trafic de stupéfiants et la prostitution. Son impact ne se limite pas aux pertes financières immédiates : elle érode la confiance dans les systèmes, exacerbe les inégalités sociales et freine le développement économique.

Ce phénomène s'est considérablement amplifié avec la démocratisation spectaculaire de l'IA générative. Les techniques utilisées sont désormais à la fois plus sophistiquées et plus accessibles au grand public. En 2024, selon le *2025 Identity Fraud Report*, les fraudes numériques ont surpassé pour la première fois les contrefaçons physiques, représentant **57% des fraudes documentaires**.

Des études récentes illustrent l'ampleur du phénomène. Selon l'étude « *Les Français et leur banque en 2024* » conduite par IN BANQUE en partenariat avec Capgemini Invent et Tessi, **17% des Français connectés** ont déjà falsifié ou modifié des documents pour faciliter l'ouverture d'un compte bancaire ou l'obtention d'un crédit. Plus alarmant encore, **ce taux monte à plus de 20% chez les moins de 35 ans**.

L'émergence de nouveaux moyens de paiement, comme les cryptomonnaies, offre également de nouvelles opportunités aux fraudeurs, facilitant des activités illicites complexes et difficiles à tracer.

En France, l'ampleur de la fraude documentaire est particulièrement préoccupante. S'il reste difficile d'en calculer le coût exact, les pertes financières dépasseraient désormais les **65 milliards d'euros annuels, soit 2,5% du PIB national**.

Le calcul de la fraude documentaire résulte de l'addition des **60 milliards €** de fraude documentaire¹ dans la fraude fiscale, des **2,7 milliards €** de fraude dans le secteur de la santé², des **2,5 milliards €** de fraude à l'assurance³, du **milliard €** de fraude bancaire⁴ et du **milliard €** de fraude du secteur immobilier⁵. À titre de comparaison, le déficit public en 2024 représentait **6,1% du PIB**.

Ce rapport propose un état des lieux détaillé des impacts de la fraude documentaire avant d'explorer des mesures concrètes pour mieux s'en prémunir.

CHIFFRES CLÉS 2024

- 100 milliards €, l'estimation de la fraude fiscale en France⁶
- + 65 milliards €, l'estimation de la fraude documentaire en France⁷
- 2,5% du PIB national impacté
- 69% des entreprises françaises ciblées⁸
- 244%⁹ d'augmentation des fraudes numériques en un an
- 17% des Français connectés ont déjà falsifié ou modifié des documents pour faciliter l'ouverture d'un compte bancaire ou l'obtention d'un crédit, et ce taux monte à plus de 20% chez les moins de 35 ans¹⁰.



La fraude documentaire est devenue une menace systémique pour notre économie. Plus qu'un enjeu de sécurité, c'est un défi sociétal qui exige une mobilisation sans précédent.

Emmanuelle Ertel,
Directrice générale d'Innovation&trust,
la digital factory de Tessi

1. 60% (2025 Identity Fraud Report) des 100 milliards de fraude fiscale totale (Rapport du Syndicat Solidaires Finances Publiques de 2019) s'appuient sur la fraude documentaire.
2. 60% des 4,5 milliards € estimés par la cour des comptes (Rapport sur l'application des lois de financement de la sécurité sociale, 2024)
3. ALFA (Association de Lutte contre la Fraude à l'Assurance)
4. Rapport Annuel de l'Observatoire de la sécurité des moyens de paiement, Banque de France (2022)

Première partie

LA FRAUDE DOCUMENTAIRE : UNE MENACE SOUS-ESTIMÉE AUX CONSÉQUENCES MAJEURES

1.1 COMPRENDRE LES MÉCANISMES DE LA FRAUDE DOCUMENTAIRE

La fraude documentaire prend des formes variées, évoluant constamment pour contourner les mécanismes de contrôle. Voici une segmentation détaillée des différentes catégories et mécanismes identifiés par l'Observatoire Tessi :

1.1.1 FRAUDE À L'IDENTITÉ :

Usurpation et falsification de documents d'identité

Cette méthode, la plus courante, repose sur la falsification ou l'usurpation d'identité. En 2022, le ministère de l'Intérieur a recensé **210 000 victimes d'usurpation d'identité en France**. Selon Europol, une grande partie des documents frauduleux détectés aux frontières de l'UE est liée à l'usurpation d'identité.

Les formes les plus répandues comprennent :

- La falsification ou contrefaçon de cartes d'identité, passeports, permis de conduire ;
- La création de fausses identités à partir de documents authentiques modifiés ;
- L'usage frauduleux de documents volés ou l'usurpation d'identité réelle.

Faux justificatifs d'identité ou de domicile

Selon LexisNexis (2021), **10 à 15% des dossiers bancaires contiennent des justificatifs falsifiés**.

Parmi les documents les plus ciblés, nous retrouvons :

- La fabrication de faux actes de naissance pour obtenir des documents officiels ;
- Le détournement ou la falsification de justificatifs de domicile (factures d'électricité, d'eau, de téléphone) pour justifier une fausse adresse.

1.1.2 FRAUDE AUX DOCUMENTS BANCAIRES ET DE PAIEMENT

Falsification de documents de crédit et de solvabilité

Ces fraudes se manifestent par :

- La création de faux bulletins de salaire pour obtenir un prêt bancaire ;
- L'usage de faux avis d'imposition pour prouver des revenus fictifs ;
- La falsification de relevés bancaires pour justifier une situation financière stable.

Dans le secteur immobilier, la fraude documentaire est particulièrement préoccupante sur le marché locatif. **Une étude d'Imodirect (février 2024) révèle que 23% des dossiers transmis par les candidats à la location en Île-de-France** comportent au moins un élément falsifié, illustrant l'ampleur du phénomène dans les zones à forte tension locative.

Cette problématique ne se limite pas au marché locatif et s'étend également au secteur du crédit immobilier. **Selon l'Agence de contrôle prudentiel et de résolution (ACPR) de la Banque de France, les fraudes liées aux faux crédits immobiliers ont connu une forte progression depuis l'été 2024, avec un préjudice estimé à plus d'un milliard d'euros au total.** Cette escroquerie, qui cible particulièrement les emprunteurs attirés par des offres de taux avantageux, touche en moyenne 12 000 euros par victime.

Usurpation de documents de paiement

Selon les chiffres de l'Observatoire de la sécurité des moyens de paiement, **la carte bancaire serait le moyen de paiement le plus fraudé, avec un montant de 251 millions d'euros (2023)**. Les techniques les plus courantes sont :

- La falsification de chèques pour réaliser des encaissements frauduleux ;
- La contrefaçon de cartes de paiement avec des données volées ;
- La création de faux IBAN pour détourner des fonds.

5. ACPR, Agence de contrôle prudentiel et de résolution (2024)

6. Rapport du Syndicat Solidaires Finances Publiques, 2019

7. Estimation de l'Observatoire Tessi, 2025

8. Étude Allianz-DFCG, 2022

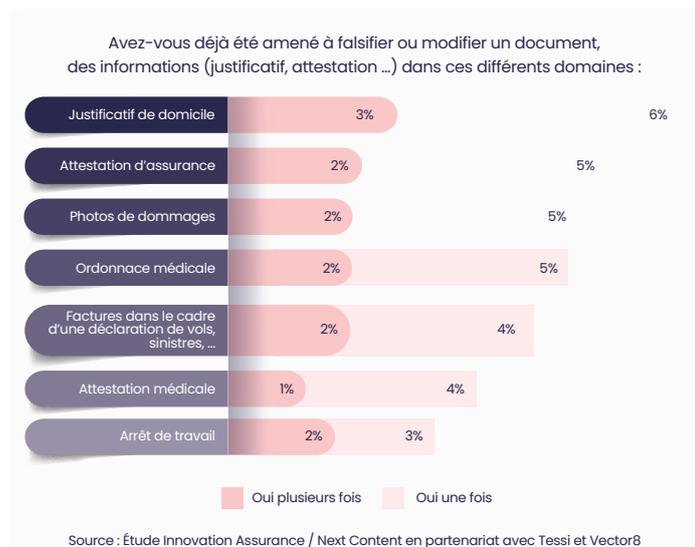
9. 2025 Identity Fraud Report

10. Étude « Les Français et leur banque en 2024 » conduite par IN BANQUE en partenariat avec Capgemini Invent et Tessi

1.1.3 FRAUDE AUX DOCUMENTS D'ASSURANCE, DE SANTÉ ET AUX AIDES SOCIALES

Falsification de documents d'assurance et de santé

La protection sociale et le secteur des assurances constituent des cibles privilégiées pour les fraudeurs. Les mécanismes de remboursement et d'indemnisation, souvent basés sur des déclarations et justificatifs fournis par les assurés eux-mêmes, présentent des vulnérabilités exploitées tant par des individus isolés que par des réseaux organisés.



Graphique 1 : Proportion d'assurés ayant déjà falsifié des documents par type

L'étude « *Innovation Assurance* » menée par Next Content en partenariat avec Tessi et Vector8 (février 2025) met en lumière que 20% des assurés français ont déclaré avoir déjà falsifié au moins un document parmi ceux couramment demandés par les assureurs.

Les pratiques les plus répandues incluent :

- L'usage de faux certificats médicaux pour bénéficier d'indemnités, arrêts maladie, ou invalidité (5% des assurés) ;
- La falsification de déclarations de sinistre pour toucher des remboursements frauduleux ;
- L'utilisation de fausses ordonnances médicales pour obtenir des médicaments contrôlés ou des remboursements (7% des assurés) ;
- La falsification de justificatifs de domicile (9% des assurés) et d'attestations d'assurance (7% des assurés).

11. PwC's Global Economic Crime and Fraud Survey 2022

Fraude aux documents administratifs et aux aides sociales

Le Haut conseil du financement de la protection sociale évalue la fraude sociale au minimum à 13 milliards d'euros (Md€) annuels.

Les exemples typiques comprennent :

- L'usage de faux certificats de résidence ou faux bulletins de salaire pour obtenir des avantages sociaux ;
- La manipulation de dossiers de naturalisation pour obtenir une nationalité induue ;
- La falsification de déclarations fiscales pour bénéficier d'exonérations injustifiées.

1.1.4 FRAUDE AUX DOCUMENTS D'ENTREPRISE ET AUX ÉCHANGES COMMERCIAUX

Faux documents comptables et fiscaux

Les pratiques les plus courantes incluent :

- La manipulation de bilans comptables pour masquer des pertes ou frauder le fisc ;
- La création de faux KBIS ou la modification de statuts pour éditer un « vrai faux KBIS » ;
- La falsification de factures pour gonfler des dépenses ou justifier de fausses transactions ;
- Les fausses déclarations de TVA avec documents justificatifs falsifiés.

Fraude aux marchés publics et subventions

D'après PwC, 46%¹¹ des organisations ont déclaré avoir subi une forme de fraude au cours des 24 derniers mois.

Les exemples courants sont :

- La production de faux dossiers de candidature avec des qualifications falsifiées ;
- La falsification de rapports d'activité pour justifier l'usage des fonds publics.

Fraude aux documents douaniers et de transport

Cette catégorie comprend notamment :

- La falsification de documents de transport et de logistique (connaissances, bons de livraison) pour détourner des marchandises ;
- La contrefaçon de déclarations douanières pour sous-évaluer des importations ou éviter des taxes ;
- La contrefaçon de certificats d'immatriculation de véhicules.

1.1.5 FRAUDE AUX DOCUMENTS LÉGAUX ET JUDICIAIRES

Fraude aux documents juridiques

Interpol indique que les faux documents légaux sont fréquemment utilisés dans les fraudes à l'identité, aux titres de propriété et aux transactions bancaires. Les manifestations courantes sont :

- La contrefaçon de contrats (bail, vente, mariage, etc.) pour tromper une administration ou un particulier ;
- La falsification de décisions de justice pour escroquer une victime ou influencer une procédure ;
- La création de faux testaments et actes notariés pour détourner des successions.

Fraude aux diplômes et qualifications

Une étude conjointe menée par Credence et Prospects, révèle que près de **50%** des grandes entreprises et des PME ont rencontré des cas de personnes ayant menti sur leurs qualifications universitaires (2021). **Selon une enquête menée par la Commission nationale de la certification professionnelle (CNCP) en 2024, environ 20 000 faux diplômes circulent en France chaque année.**

Les exemples typiques comprennent :

- La contrefaçon de diplômes universitaires pour accéder à des postes qualifiés ;
- La falsification de certificats de formation pour obtenir une promotion ou un emploi ;
- L'usage de titres professionnels usurpés (médecins, avocats, ingénieurs, agents immobiliers) ;
- L'utilisation de faux permis de travail pour employer ou travailler illégalement.

Fraude aux attestations, certifications et brevets

Europol signale de nombreuses contrefaçons de certifications techniques et brevetées, notamment dans l'industrie et la recherche. Ces fraudes incluent :

- La contrefaçon de labels de conformité (ex. : CE, ISO) pour vendre des produits non conformes ;
- La falsification de certificats environnementaux pour bénéficier de subventions écologiques ;
- La falsification ou création de faux brevets.

1.2. UN IMPACT ÉCONOMIQUE MASSIF ET SOUS-ÉVALUÉ

Les répercussions économiques de la fraude documentaire sont vastes et concernent plusieurs niveaux.

Un poids sur l'économie nationale : impact sur le PIB et pertes sectorielles

Les pertes financières liées à la fraude documentaire dépassent désormais **65 milliards d'euros par an, soit 2,5% du PIB national**. L'ampleur de ce phénomène affecte directement les budgets alloués à des politiques publiques cruciales, comme la santé ou l'éducation, fragilisant ainsi l'ensemble de l'économie nationale.

Une enquête récente d'Allianz x DFCG, dresse un constat alarmant : **69% des entreprises françaises ont été visées par au moins une tentative de fraude documentaire en 2022**. La situation est encore plus critique pour les grandes entreprises, ce chiffre atteignant 91% pour celles réalisant un chiffre d'affaires supérieur à 100 millions d'euros. L'impact peut être dévastateur, avec des pertes pouvant atteindre jusqu'à 7% du chiffre d'affaires.

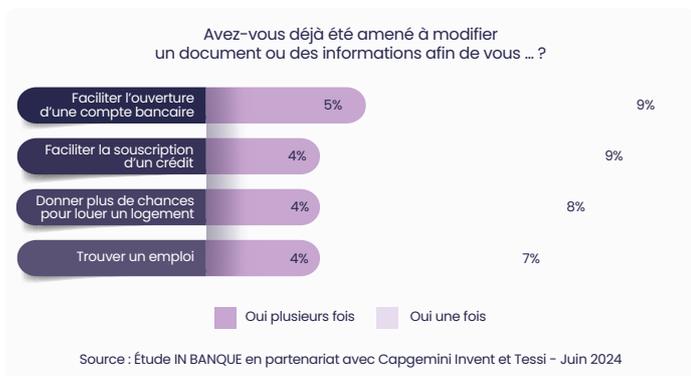
Cette menace multiforme génère des répercussions qui vont bien au-delà des pertes financières directes. Les dommages réputationnels affectent durablement la confiance des clients, des partenaires commerciaux et des investisseurs. Cette érosion de la confiance crée un effet domino : **réticence à conclure des accords, refus d'investissement, fragilisation de la capacité de l'entreprise à lever des fonds et à se développer.**

Face à ces enjeux, les entreprises sont contraintes de réagir : **selon une étude, 80% des responsables de la lutte contre la fraude confirment l'existence d'une cellule anti-fraude au sein de leur organisation**. Paradoxalement, les mesures de sécurité rigoureuses mises en place pour se prémunir des tentatives de fraudes finissent souvent par ralentir les processus opérationnels, générant des coûts indirects significatifs.

Un risque accru pour les institutions financières

Le secteur financier est particulièrement vulnérable à la fraude documentaire, avec des pertes significatives et des mécanismes de fraude de plus en plus sophistiqués. **Le secteur bancaire français a ainsi enregistré plus de 1 milliard d'euros de pertes en 2023¹², avec une moyenne inquiétante de 4 200 euros par fraude réussie.**

12. Rapport de l'Observatoire de la sécurité des moyens de paiement 2023



Graphique 2 : Proportion de Français ayant déjà falsifié des documents dans le domaine bancaire

Deux types principaux de fraudes menacent les établissements bancaires. D'une part, les fraudes à la souscription, qui visent à obtenir des produits ou services bancaires sur la base de faux documents. D'autre part, les fraudes au financement, particulièrement préoccupantes dans le cadre de la Lutte contre le Blanchiment d'argent et le Financement du Terrorisme (LCB-FT).

L'étude « *Les Français et leur banque en 2024* », conduite par IN BANQUE en partenariat avec Capgemini Invent et Tessi, **révèle que 14% des Français connectés auraient déjà falsifié des documents pour faciliter l'ouverture d'un compte bancaire et 13% pour obtenir un crédit. Au total, 17% ont fait au moins l'une des deux démarches.**

La situation s'aggrave : la Banque de France (2023) signale une augmentation alarmante de **37%** des fraudes liées aux moyens de paiement, contraignant les établissements à investir massivement dans la sécurisation de leurs processus.

Le secteur assurantiel n'est pas épargné, avec **2,5 milliards d'euros de pertes annuelles**¹³.

Plus inquiétant encore, les fraudes à l'assurance et à la garantie affichent des taux de réussite particulièrement élevés, atteignant **80%**¹⁴ des cas. L'étendue de la fraude témoigne d'une industrialisation des pratiques frauduleuses qui, bien que portant sur des montants unitaires plus modestes que dans le secteur bancaire, génèrent des pertes massives par leur volume.

¹³. Lutte contre la Fraude à l'Assurance (ALFA)

¹⁴. Étude Selvitys 2024

Le coût de la conformité : l'impact des obligations KYC sur les entreprises

Au-delà des pertes directes causées par la fraude, les entreprises font face à un autre défi économique majeur : **le coût de la conformité réglementaire**. Les obligations légales en matière de vérification d'identité, connues sous l'acronyme KYC (« Know Your Customer »), imposent désormais des contrôles stricts pour lutter contre la fraude documentaire et le blanchiment d'argent. Ces obligations engendrent des coûts indirects non négligeables pour les entreprises, tels que les investissements en technologies et les charges opérationnelles liées aux vérifications accrues.

En effet, ces obligations nécessitent souvent des dispositifs complexes impliquant des vérifications approfondies de documents multiples (**pièces d'identité, justificatifs de domicile, avis d'imposition, bulletins de salaire...**). Les entreprises, et particulièrement les banques, doivent investir massivement pour automatiser ces vérifications. Ces investissements permettent toutefois de réduire considérablement les risques financiers et réputationnels, en évitant notamment les amendes conséquentes associées à une non-conformité.

Dans ce contexte, **les nouvelles solutions technologiques permettent aujourd'hui d'automatiser jusqu'à 80% des contrôles documentaires et d'accroître la productivité opérationnelle de 25%**. Les entreprises disposent ainsi d'outils capables de détecter rapidement les modifications frauduleuses grâce à l'intelligence artificielle et aux contrôles croisés, réduisant significativement les coûts liés à la gestion manuelle et les risques associés.

L'impact sur le e-commerce et la distribution

Le commerce électronique est devenu une cible privilégiée pour les fraudeurs.

Selon le *Retail Report 2024* publié par Adyen, le coût annuel de la fraude dans le secteur de la distribution atteint, rien qu'en France, 17 milliards d'euros. Ce montant, qui excède à lui seul le budget du ministère en charge de la Transition écologique, s'inscrit en progression constante (+56% sur un an). Face à cette menace, les commerçants se retrouvent dans un dilemme complexe : **renforcer les contrôles pour limiter les pertes ou privilégier la fluidité du parcours client pour maximiser les ventes.**

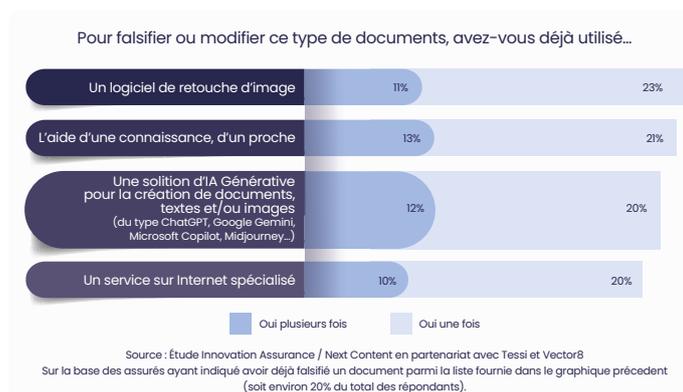
L'intelligence artificielle, une menace émergente à l'assaut de l'économie

L'année 2024 marque un tournant dans l'évolution de la fraude documentaire, avec l'émergence de nouvelles menaces portées par les avancées technologiques. **Entre 2023 et 2024, la falsification de documents numériques a connu une hausse vertigineuse de 244%, signalant une véritable industrialisation des pratiques frauduleuses.**

L'utilisation massive de l'Intelligence Artificielle a profondément transformé les techniques de fraude documentaire. Aujourd'hui, les fraudeurs utilisent couramment des outils numériques sophistiqués pour créer des faux réalistes en grande quantité, une tendance renforcée par l'accès facile aux sites internet spécialisés et aux solutions d'IA générative grand public.

L'intelligence artificielle générative joue un rôle prépondérant dans cette transformation.

Dans le secteur bancaire, le rapport *Signicat* révèle que **42,5% des fraudes sont désormais générées par l'IA, avec un taux de réussite préoccupant de 29%.**



Graphique 3 : Solutions technologiques utilisées pour falsifier des documents

L'IA générative et les logiciels de retouche d'image sont devenus les outils privilégiés des fraudeurs. L'étude « *Innovation Assurance* » menée par Next Content en partenariat avec Tessi et Vector8 (février 2025), révèle que parmi les personnes ayant déjà falsifié des documents, **34% ont utilisé un logiciel de retouche d'image, 32% ont eu recours à une solution d'IA générative (du type ChatGPT, Google Gemini, Microsoft Copilot, Midjourney...), et 30% ont utilisé un site internet spécialisé.**

De nombreux fraudeurs cumulent l'usage de plusieurs solutions, tandis que d'autres (34%) s'appuient sur l'aide d'un proche. **Ces outils numériques de falsification concernent désormais entre 5 et 6% du total des assurés interrogés,** démontrant la démocratisation inquiétante de ces pratiques.



Les fraudeurs adaptent leurs techniques à une vitesse alarmante. Ces menaces sont omniprésentes et touchent tous les secteurs, des entreprises aux gouvernements, en passant par les particuliers.



Simon Horswell,

Spécialiste de la fraude chez Entrust

L'émergence des deepfakes illustre parfaitement cette sophistication technologique. Grâce à des algorithmes d'analyse massive de données (vidéos, photos), **les fraudeurs peuvent désormais recréer ou manipuler des visages de façon ultra-réaliste, rendant la détection des fraudes toujours plus complexe.**

La diversification des pratiques de fraude via l'IA s'accompagne d'une prolifération des supports falsifiés les plus couramment ciblés : **cartes d'identité, passeports, bulletins de salaire, justificatifs de domicile, relevés bancaires, avis d'imposition et ordonnances médicales,** autant de documents désormais vulnérables.



1.3. POURQUOI LA FRAUDE PROSPÈRE : MOTIVATIONS ET FACTEURS AGGRAVANTS

Les nouvelles technologies facilitent indéniablement la fraude documentaire, mais ce sont les motivations humaines et les failles systémiques qui expliquent sa progression constante, créant un terreau favorable à son développement.

Les motivations financières

L'étude *Selvitys* 2024 dresse un portrait nuancé des motivations qui poussent à la fraude documentaire.

La précarité économique apparaît comme le premier facteur déclencheur : 38% des fraudeurs citent le manque de ressources comme principale motivation. Cette statistique souligne le lien étroit entre les difficultés financières et le passage à l'acte, particulièrement dans un contexte économique tendu.

Cependant, les motivations ne se limitent pas aux seules contraintes économiques.

L'étude révèle qu'un tiers des fraudeurs (33%) agissent par sentiment d'impunité, convaincus que les systèmes de détection présentent suffisamment de failles pour échapper aux sanctions. Ce sentiment est renforcé par des contrôles souvent perçus comme insuffisants ou mal coordonnés.

Le sentiment d'impunité

La méconnaissance des risques légaux joue un rôle crucial dans la prolifération des fraudes. **Seuls 31% des fraudeurs se déclarent pleinement informés des sanctions qu'ils encourent.** Cette ignorance crée un terreau favorable à la prise de risque, même si paradoxalement, **55% des fraudeurs admettent ressentir de l'anxiété face aux conséquences potentielles de leurs actes.**

Les disparités de genre dans la perception du risque sont particulièrement marquées :

39% des hommes fraudeurs minimisent les répercussions possibles, contre seulement 21% des femmes. Cette différence significative suggère que les stratégies de prévention pourraient bénéficier d'une approche plus ciblée selon les profils.

Ces disparités de genre sont également confirmées par l'étude « *Innovation Assurance* » menée par Next Content en partenariat avec Tessi et Vector8 (février 2025), qui révèle **que les hommes fraudent systématiquement plus que les femmes, quel que soit le type de document, avec un écart de 1 à 2 points de pourcentage.** L'étude « *Les Français et leur banque en 2024* », conduite par IN BANQUE

en partenariat avec Capgemini Invent et Tessi, va plus loin et montre des écarts encore plus marqués : **16% des hommes ont falsifié des documents pour obtenir un crédit contre seulement 9% des femmes, et 17% contre 11% pour l'ouverture d'un compte bancaire.**

La démocratisation de la « fraude amicale »

Au-delà des motivations économiques et du sentiment d'impunité déjà évoqués, on observe une démocratisation inquiétante de ce que les experts nomment la « fraude amicale » (friendly fraud). **Ce phénomène, particulièrement répandu dans le commerce en ligne, consiste pour des consommateurs ordinaires à abuser des conditions générales de vente : déclaration mensongère de non-réception de commande, demande de remboursement, suivi du renvoi d'un colis vide ou contenant un produit différent de l'original.**

Plus alarmant encore, des « services » proposés sur le Dark Web et les réseaux sociaux permettent désormais, moyennant commission, d'aider des consommateurs ordinaires à commettre ces fraudes. **Selon une étude de Riskified, le coût mondial de ces pratiques atteindrait 28,4 milliards de dollars.**

Les conséquences sur la société

Au-delà des motivations individuelles, la fraude documentaire révèle une fracture sociale plus profonde. **Un quart des fraudeurs (25%) justifient leurs actes par un sentiment d'injustice sociale, transformant la fraude en une forme de rébellion contre les institutions.**

Cette dimension politique de la fraude appelle à une réponse qui dépasse le simple cadre répressif pour inclure des actions de sensibilisation et d'éducation visant à restaurer la confiance dans les systèmes établis.

La banalisation de la fraude constitue peut-être le signal le plus alarmant. **Quand 10,8% des Français admettent avoir déjà utilisé un faux document, avec un taux de réussite de 73%, cela témoigne d'une normalisation inquiétante de ces pratiques.** Plus préoccupant encore, les jeunes de 18-24 ans montrent une propension accrue à considérer la fraude comme une option acceptable, laissant présager un défi majeur pour les années à venir.

L'appât du gain pur, bien que minoritaire (12% des cas), ne doit pas être négligé. Il traduit une forme de déconnexion morale où la fraude devient un simple calcul d'opportunité, détaché de toute considération éthique ou sociale.

Face à ces différentes motivations, la prévention de la fraude documentaire nécessite une approche globale, combinant répression, éducation et réduction des inégalités sociales.

1.4. UNE MENACE SANS FRONTIÈRES

La fraude documentaire est un phénomène mondial, avec des manifestations variées selon les régions.

Royaume-Uni

La **National Crime Agency (NCA)** rapporte une augmentation alarmante des cas d'usurpation d'identité, en particulier dans les secteurs des télécommunications et des services publics. Cela illustre une adaptation rapide des fraudeurs à la numérisation croissante.

L'Italie

Une étude de l'**ABI (Associazione Bancaria Italiana)** révèle que les prêts hypothécaires sont particulièrement visés, avec une augmentation de 42% des fraudes documentaires en 2023. Cela démontre l'attrait des secteurs où de fortes sommes sont en jeu.

Les États-Unis

Le système d'identification sociale est fréquemment ciblé par des faux documents, permettant aux fraudeurs de bénéficier de prestations sociales indues. Les autorités renforcent leurs systèmes de vérification, mais le défi reste complexe, en raison de l'échelle des opérations frauduleuses.

Le reste du monde : hors Union européenne et États-Unis

Parmi les documents les plus ciblés par la fraude numérique figurent **le numéro fiscal indien (27%) et les cartes d'identité nationale du Pakistan (18%) et du Bangladesh (15%)¹⁵.**

10,8% des Français admettent avoir déjà utilisé un faux document, avec un taux de réussite de 73%

15. 2025 Identity Fraud Report

Deuxième partie

Deuxième partie

ANTICIPER ET CONTRER LA FRAUDE

2.1 QUE DIT LA LOI

LA LÉGISLATION FRANÇAISE :

La fraude documentaire en France est principalement régie par les dispositions du Code pénal, notamment les articles 441-7, 441-8, 441-9 et 441-10. Ces articles encadrent les infractions liées à l'usage frauduleux de documents, leur falsification ou leur établissement inexact.

- **Usage frauduleux de documents :**
l'article 441-8 du Code pénal incrimine l'utilisation de documents appartenant à un tiers (pièces d'identité, titres de séjours), dans le but d'entrer, de circuler ou de se maintenir sur le territoire français, ou encore d'obtenir indûment un titre, une qualité, un statut ou un avantage.
Cette infraction est punie de cinq ans d'emprisonnement et de 75 000 euros d'amende. Les peines sont portées à sept ans d'emprisonnement et 100 000 euros d'amende en cas de récidive ou d'infractions commises de manière habituelle.
- **Établissement ou falsification de documents :**
l'article 441-7 du Code pénal réprime l'établissement ou la falsification d'attestations ou certificats inexacts, ainsi que leur usage.
Les peines encourues sont d'un an d'emprisonnement et de 15 000 euros d'amende, mais elles peuvent être portées à trois ans d'emprisonnement et 45 000 euros d'amende si ces infractions visent à obtenir un titre de séjour ou une protection contre l'éloignement.
- **Tentative et peines complémentaires :**
la tentative de fraude documentaire est également punissable des mêmes peines selon l'article 441-9 du Code pénal. En outre, des peines complémentaires peuvent être prononcées, telles que l'interdiction des droits civiques, l'interdiction d'exercer certaines fonctions ou professions, ou encore la confiscation des objets ayant servi à commettre l'infraction.

LA LÉGISLATION EUROPÉENNE :

Au niveau européen, la lutte contre la fraude documentaire s'inscrit dans un cadre de coopération entre les États membres, notamment pour prévenir et sanctionner les infractions transfrontalières.

- **Directive DAC 6 et dispositifs transfrontières :**
la directive DAC 6, transposée en France par l'ordonnance n°2019-1068 du 21 octobre 2019, **impose une obligation déclarative pour les dispositifs transfrontières présentant des marqueurs de fraude ou d'évasion fiscale.** Ces dispositifs doivent être déclarés par les intermédiaires ou les contribuables concernés, et les informations sont échangées automatiquement entre les États membres («L'article 22 de la loi n° 2018-898 du 23 octobre 2018 relative à la lutte contre la fraude a autorisé le Gouvernement à prendre par voie d'ordonnance les mesures [...] propres à transposer la directive DAC 6»).
- **Rôle de l'OLAF (Office européen de lutte antifraude) :**
l'OLAF joue un rôle central dans la lutte contre la fraude documentaire en Europe. Il coopère avec les autorités nationales pour enquêter sur les cas de fraude impliquant des fonds européens. Par exemple, dans une affaire de détournement de fonds liés à un programme d'échanges d'étudiants, l'OLAF a collecté des preuves transnationales et soutenu les poursuites judiciaires dans les États membres concernés.
- **Partenariat avec le Parquet européen :**
le Parquet européen, en collaboration avec l'OLAF, Europol et Eurojust, vise à renforcer la lutte contre la fraude documentaire et les infractions transfrontalières. Ce partenariat permet une meilleure coordination des enquêtes et des poursuites judiciaires dans les affaires complexes impliquant plusieurs États membres.

2.2. UNE ÉVOLUTION DU CADRE LÉGAL QUI S'IMPOSE

Pour lutter efficacement contre la fraude documentaire, une adaptation et un renforcement des cadres juridiques sont indispensables.

• En France

Le Rapport d'information du Sénat (2019) souligne l'importance d'une collaboration accrue entre les acteurs publics et privés. Les dispositifs législatifs actuels doivent être complétés par des mécanismes de partage de données, garantissant un suivi plus rigoureux des fraudes. Cela pourrait inclure la création de bases de données interconnectées pour détecter les anomalies.

La proposition de loi visant à sortir la France du piège du narcotrafic qui sera prochainement débattue au Sénat¹⁶ prévoit en son article 4 une future « présomption de blanchiment » pour les transactions en cryptomonnaies.

• Au niveau européen

L'Union européenne pourrait tirer parti d'une base de données commune pour permettre une vérification rapide et sécurisée des documents.

Cette recommandation vise à harmoniser les pratiques entre les États membres, en réduisant les disparités et en facilitant les enquêtes transfrontalières.

• Aux États-Unis

Si le Patriot Act a permis d'imposer des exigences strictes en matière de vérification d'identité dans les institutions financières, des failles subsistent. Les secteurs non bancarisés, où les contrôles sont moins fréquents, représentent une opportunité pour les fraudeurs. Un renforcement de la réglementation dans ces domaines pourrait limiter ces vulnérabilités.

2.3. COMMENT LES ENTREPRISES PEUVENT MIEUX SE PROTÉGER

4 BONNES PRATIQUES À ADOPTER

- Digitalisation des contrôles
- Formation continue des équipes
- Politique de vérification systématique
- Audits réguliers



L'étude *Selvitys* pour Finovox rapporte que 80% des répondants considèrent la lutte contre la fraude comme l'un de leurs 3 enjeux principaux. Cette priorité se pose même avec une acuité plus forte pour les entreprises de plus de 100 personnes où 80% des responsables voient comme essentielle la lutte contre la fraude (contre 60% pour les entreprises comptant plus de 20 salariés).

Des mesures opérationnelles adaptées peuvent réduire considérablement les risques :

Digitalisation des processus

Selon le *Rapport Selvitys* (2024), l'utilisation de solutions d'intelligence artificielle pour automatiser les contrôles documentaires constitue une avancée majeure. Ces outils permettent de détecter des anomalies complexes, tout en réduisant la dépendance aux évaluations manuelles, souvent sujettes à des erreurs. Une plateforme de détection automatisée peut analyser des milliers de documents en quelques minutes, identifiant des incohérences invisibles à l'œil humain.

Formations spécifiques

Bien que 80% des entreprises, victimes de tentative de fraude, françaises disposent d'une cellule anti-fraude, ces équipes doivent être formées en continu. **Les techniques des fraudeurs évoluant rapidement, une mise à jour régulière des compétences et des outils utilisés est essentielle pour maintenir une défense efficace.** Les programmes de formation doivent inclure à la fois les aspects techniques (reconnaissance des fraudes) et les compétences comportementales (détection des signaux d'alerte).

16. <https://www.senat.fr/leg/pp123-735.pdf>

Politiques internes rigoureuses

Les entreprises doivent s'assurer de vérifier systématiquement les documents transmis par leurs fournisseurs et clients. Cela peut inclure des **audits réguliers, des protocoles de validation renforcés et une standardisation des processus de contrôle**. L'établissement de procédures claires et documentées permet d'assurer la cohérence des vérifications et d'éviter les failles dans le système de contrôle.

Veille technologique permanente

Face à l'évolution rapide des technologies utilisées par les fraudeurs, les entreprises doivent maintenir une veille constante sur les nouvelles méthodes de fraude et les contre-mesures disponibles. Cette vigilance doit s'accompagner d'une capacité à déployer rapidement de nouvelles solutions de protection en réponse aux menaces émergentes.

Stratégies spécifiques adoptées par le secteur du e-commerce

Le secteur du e-commerce, particulièrement exposé aux nouvelles formes de fraude, a développé des approches multidimensionnelles combinant solutions technologiques et mesures opérationnelles.

Sur le plan technologique, de nombreux commerçants en ligne ont déployé des systèmes de détection en temps réel s'appuyant sur le big data et l'intelligence artificielle. Ces outils analysent le comportement d'achat de chaque client pour identifier, à partir d'une série de paramètres (vitesse de navigation, rythme de saisie, etc.), si une transaction présente des caractéristiques suspectes par rapport à l'historique de l'utilisateur.

Parallèlement, pour lutter contre la 'fraude amicale' qui prolifère dans les retours de produits, les e-commerçants ont dû mettre en place des politiques de retour plus strictes. **Ces mesures organisationnelles, bien que potentiellement préjudiciables à l'expérience client, s'avèrent nécessaires face à l'ampleur du phénomène :**

- **1/3** des détaillants appliquent désormais des frais postaux pour tous les renvois ;
- Une proportion similaire (**33%**) ne rembourse plus en numéraire mais propose uniquement des échanges ou des avoirs ;
- **38%** d'entre eux exigent un dépôt de plainte préalable dans les cas où le client déclare sa commande volée.

Ces mesures illustrent le délicat équilibre que les entreprises doivent trouver entre la protection contre la fraude et le maintien d'une expérience client fluide. Comme le témoigne un responsable de la lutte contre la fraude d'un grand groupe de distribution :

Entre le fait que les clients n'ont pas toujours à proximité leur appareil de confiance pour s'authentifier et les incidents de réseau Internet, [...] l'entreprise doit parvenir à un équilibre subtil entre, d'une part, la faculté à proposer un parcours client le plus fluide possible, sans friction, pour maximiser les ventes, et, d'autre part, la lutte contre la fraude, qui génère des pertes et vient ainsi grever la marge opérationnelle.¹⁷

Témoignage anonyme d'un responsable de la lutte contre la fraude d'un grand groupe de distribution.

Des services innovants comme les garanties de « rétrofacturation », fournies par des prestataires spécialisés en prévention de la fraude, suscitent également un intérêt croissant. Ces solutions viennent couvrir le marchand contre des transactions frauduleuses préalablement validées par ces prestataires, offrant ainsi une protection financière face aux pertes potentielles.

2.4. LES SOLUTIONS TECHNOLOGIQUES POUR LUTTER CONTRE LA FRAUDE DOCUMENTAIRE

La lutte contre la fraude documentaire s'appuie aujourd'hui sur des technologies de pointe qui permettent une détection plus efficace et une prévention renforcée des tentatives de fraude.

Solutions d'authentification avancée

L'authentification biométrique représente une avancée majeure dans la fiabilité de la vérification des identités. **Selon le cabinet MarketsandMarkets¹⁸, la taille du marché mondial des systèmes biométriques devrait atteindre 84,5 milliards USD d'ici 2029, avec un taux de croissance annuel composé (CAGR) de 12,3 % pendant la période de prévision de 2024 à 2029.** Les solutions biométriques connaissent un essor considérable, portées par une demande croissante de sécurité renforcée dans un contexte de digitalisation accélérée.

¹⁷. Citation tirée de l'article « Commerce en ligne : la fraude prend de nouvelles formes », Option Finance, 2025

¹⁸. Biometric System Market by Authentication Type – Global Forecast to 2029

Ces solutions combinent plusieurs facteurs :

La reconnaissance faciale

L'analyse des empreintes digitales

La reconnaissance vocale

La détection du vivant
(« liveness detection »)



La combinaison de ces différentes technologies permet une identification plus fiable et réduit significativement les risques d'usurpation d'identité.

Intelligence Artificielle & Machine Learning

Les solutions basées sur l'IA constituent désormais un pilier essentiel de la lutte anti-fraude :

• Analyse comportementale :

les algorithmes de machine learning permettent de détecter des schémas suspects dans les transactions et les comportements des utilisateurs. Ces systèmes s'adaptent en permanence aux nouvelles menaces.

• Vérification automatisée des documents :

les technologies de computer vision peuvent analyser en temps réel l'authenticité des documents soumis, en vérifiant :

- » La cohérence des polices utilisées ;
- » La présence des éléments de sécurité requis ;
- » La qualité des hologrammes et filigranes ;
- » Les modifications potentielles du document.

Blockchain & traçabilité

La technologie blockchain émerge comme une solution prometteuse pour sécuriser les documents sensibles. Selon une étude IDC (2023), **35%** des institutions financières européennes expérimentent déjà cette technologie pour la vérification documentaire.

Ses principaux avantages sont :

- L'immutabilité des données enregistrées ;
- La traçabilité complète des modifications ;
- La décentralisation qui rend la falsification plus complexe ;
- La possibilité de créer des « smart contracts » pour automatiser les vérifications.

Solutions hybrides et approche multianale

Les experts recommandent une approche combinant plusieurs technologies de vérification :

- La vérification biométrique ;
- L'analyse documentaire par IA ;
- L'authentification via blockchain ;
- Des contrôles humains ciblés.

Cette approche multicouche permet d'atteindre des taux de détection supérieurs à **99%** selon les tests **indépendants réalisés par l'ANSSI en 2023**.

Face à la sophistication croissante des méthodes de fraude, l'étude IN BANQUE, sur « *Les Français et leur banque en 2024* », réalisée en partenariat avec Capgemini Invent et Tessi, souligne l'importance des solutions d'authentification innovantes comme France Connect. L'étude révèle que parmi les utilisateurs de ce service, **53%** seraient prêts à l'utiliser pour s'authentifier et éviter d'envoyer des pièces justificatives lors de l'ouverture d'un compte ou la souscription d'un crédit (dont **23%** se déclarent « certains » de l'utiliser). Ce type de vérification directe à la source constitue une réponse prometteuse face à la vulnérabilité des documents traditionnels.

Open Banking et Open Data

Les approches basées sur l'Open Banking et l'Open Data représentent une avancée significative dans la vérification documentaire. **En permettant l'accès direct et sécurisé aux données à leur source, ces technologies éliminent le besoin de documents intermédiaires susceptibles d'être falsifiés.** Par exemple, au lieu de demander un relevé bancaire qui pourrait être manipulé, une institution peut, avec l'autorisation du client, accéder directement aux données bancaires authentiques via des API sécurisées. Cette approche réduit considérablement les risques de fraude tout en simplifiant l'expérience utilisateur.

LE PORTEFEUILLE D'IDENTITÉ NUMÉRIQUE EUROPÉEN (EUDI WALLET)

La Commission européenne a lancé l'initiative du portefeuille d'identité numérique européen (EUDI Wallet) dans le cadre de la révision du règlement eIDAS. **Ce dispositif, dont le déploiement est prévu à l'horizon 2026, représente une avancée majeure dans la lutte contre la fraude documentaire.** Il permettra à chaque citoyen européen de stocker de manière sécurisée ses documents d'identité et ses attestations numériques (diplômes, certificats médicaux, permis de conduire, etc.) dans une application unique reconnue dans tous les États membres.

Sa force réside dans son principe d'attestations vérifiables émises directement par des autorités compétentes et vérifiables par un tiers via une infrastructure de confiance décentralisée.

Pour les entreprises et administrations, ce dispositif simplifiera considérablement les processus de vérification tout en renforçant leur fiabilité. Les secteurs fortement exposés à la fraude documentaire, comme la banque et l'assurance, pourront ainsi accéder à des données certifiées à la source plutôt que de s'appuyer sur des documents potentiellement falsifiés.

L'EUDI Wallet fonctionnera comme un coffre-fort numérique personnel, permettant aux utilisateurs de prouver leur identité et de partager des informations certifiées sans présenter de documents physiques, réduisant ainsi drastiquement les risques de falsification.

Limites et perspectives

Si ces solutions technologiques sont prometteuses, elles présentent également certaines limitations :

- **Coûts d'implémentation :**
l'investissement initial peut être conséquent, particulièrement pour les PME ;
- **Complexité technique :**
la maintenance et la mise à jour de ces systèmes requièrent une expertise spécifique ;
- **Protection des données :**
la conformité au RGPD doit être assurée, notamment pour les données biométriques ;
- **Limites de l'Open Banking :**
selon des experts, environ 50% des clients sont réticents à partager leurs informations d'identification, ce qui peut freiner l'adoption généralisée de ces solutions, malgré une réduction considérable des risques de fraude et une simplification de l'expérience utilisateur pour ceux qui l'adoptent ;
- **Contraintes de la Blockchain :**
cette technologie nécessite que les documents soient disponibles dans leur format natif (PDF d'origine). Dans la plupart des cas, les clients envoient des documents rescannés, perdant alors la possibilité de fonctionner en Blockchain, ce qui constitue un obstacle significatif à l'adoption généralisée de cette solution ;
- **Limites du Wallet européen :**
son caractère facultatif pour les citoyens implique que les fraudeurs ne l'utiliseront pas. La courbe de montée en force de l'utilisation sera très lente ;
- **Course technologique :**
les fraudeurs développent constamment de nouvelles techniques pour contourner ces protections.

Les experts s'accordent sur la nécessité d'une veille technologique constante et d'une adaptation continue des solutions de protection pour maintenir leur efficacité face à l'évolution des menaces.

2.5 L'IMPORTANCE DE LA SENSIBILISATION ET DE LA COOPÉRATION INTERSECTORIELLE

La lutte contre la fraude documentaire ne peut être pleinement efficace sans une sensibilisation accrue et une collaboration étendue entre les secteurs :

Informer et responsabiliser

L'Observatoire Tessi, spécialisé dans l'analyse des fraudes documentaires, pourrait jouer un rôle déterminant en organisant des ateliers pédagogiques. Ces sessions viseraient à informer les participants des risques actuels et des moyens de les prévenir. La sensibilisation doit cibler à la fois les entreprises, les administrations et le grand public pour créer une culture de vigilance collective.

Des campagnes d'information régulières sur les risques et les conséquences légales de la fraude documentaire peuvent contribuer à réduire significativement la propension à falsifier des documents. En effet, comme l'a montré notre analyse des motivations, la méconnaissance des risques légaux est un facteur important dans la décision de frauder.

Créer des réseaux d'échange

Des initiatives similaires au réseau SWIFT, qui centralise les données sur les transactions dans le secteur bancaire, pourraient être déployées dans d'autres secteurs. Ces réseaux faciliteraient le partage d'informations entre entreprises, régulateurs et autorités, permettant une détection rapide des schémas frauduleux.

La création de plateformes sectorielles dédiées au partage d'informations sur les tentatives de fraude permettrait d'alerter rapidement l'ensemble des acteurs concernés et de mettre en commun les bonnes pratiques. Cette approche collaborative est particulièrement efficace face à des menaces qui évoluent constamment et rapidement.

Former les professionnels

La formation continue des professionnels chargés de vérifier les documents est cruciale.

Ces formations doivent couvrir à la fois les aspects techniques (reconnaissance des éléments de sécurité, détection des falsifications) et comportementaux (identification des signaux d'alerte, gestion des situations suspectes).

Des programmes de certification pourraient être mis en place pour garantir un niveau de compétence homogène parmi les professionnels chargés de la vérification documentaire, créant ainsi un standard de qualité reconnu.

Conclusion

La fraude documentaire, amplifiée par la transformation numérique et l'IA générative, représente aujourd'hui un risque systémique pour l'ensemble des acteurs économiques.

Cette menace transcende les frontières sectorielles et institutionnelles, affectant aussi bien le secteur bancaire que les domaines de la santé, de l'immobilier et des services publics.



Pour relever ce défi, une approche globale s'impose. **Les solutions technologiques émergentes, comme l'authentification biométrique, l'Intelligence Artificielle ou le portefeuille d'identité numérique européen (EUDI Wallet), offrent des perspectives prometteuses.** Néanmoins, elles ne peuvent être pleinement efficaces qu'accompagnées d'un renforcement des cadres réglementaires et d'une sensibilisation accrue des acteurs.

Si l'avenir technologique est porteur d'espoir, nous devons composer avec une période transitoire où coexisteront systèmes traditionnels et innovants, créant de potentielles vulnérabilités. Les disparités réglementaires internationales et la fracture numérique constituent également des défis majeurs à surmonter. **Mais c'est par une mobilisation collective – entreprises, institutions publiques et citoyens – que nous parviendrons à édifier un environnement numérique plus sûr et plus fiable.**



La lutte contre la fraude documentaire n'est plus une option, c'est une nécessité vitale pour la survie de notre économie numérique.



Virginie Degeorgis,
Directrice générale - Tessi France



Glossaire

Glossaire de la Fraude Documentaire

A

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

C

Cryptomonnaie : Monnaie numérique décentralisée utilisant la cryptographie pour sécuriser les transactions.

Cellule anti-fraude : Service dédié au sein d'une organisation chargé de détecter, prévenir et lutter contre les tentatives de fraude.

D

Dark Web : Partie d'Internet accessible uniquement via des navigateurs spécialisés, souvent utilisée pour des activités illégales.

Deepfake : Technique utilisant l'intelligence artificielle pour créer des contenus audiovisuels truqués très réalistes.

Directive DAC 6 : Directive européenne imposant une obligation déclarative pour les dispositifs transfrontières présentant des risques de fraude fiscale.

F

Fraude à la souscription : Obtention frauduleuse de produits ou services bancaires sur la base de faux documents.

Fraude au financement : Utilisation de documents falsifiés pour obtenir des financements de manière illégale.

Fraude au faux fournisseur : Technique consistant à se faire passer pour un fournisseur légitime afin d'obtenir des paiements frauduleux.

I

IA générative : Intelligence artificielle capable de créer du contenu original, notamment des documents falsifiés.

K

KYC (Know Your Customer) : Processus de vérification de l'identité des clients, particulièrement important dans le secteur financier.

L

LCB-FT : Lutte Contre le Blanchiment d'argent et le Financement du Terrorisme.

O

OLAF : Office européen de lutte antifraude, chargé de protéger les intérêts financiers de l'Union européenne.

P

Parquet européen : Institution de l'UE chargée d'enquêter et de poursuivre les infractions pénales affectant les intérêts financiers de l'Union.

R

Rétrofacturation ou Chargeback : Procédure permettant à un consommateur ayant payé par carte bancaire d'annuler son paiement et d'être remboursé directement et gratuitement par l'émetteur de la carte ou sa banque, lorsqu'un professionnel, français ou étranger, ne respecte pas les droits du consommateur.

RGPD : Règlement Général sur la Protection des Données, cadre européen pour la protection des données personnelles.

S

Smart Contract : Contrat qui s'exécute automatiquement lorsque les clauses préalablement définies sont remplies grâce à une technologie informatique. L'intérêt initial d'y avoir recours consiste en l'automatisation du tiers de confiance, s'appuyant ainsi sur la transparence et l'immutabilité de la blockchain.

SWIFT : Society for Worldwide Interbank Financial Telecommunication, réseau de messagerie sécurisée pour les transactions financières internationales.

U

Usurpation d'identité : Utilisation frauduleuse de l'identité d'une autre personne pour commettre des actes illégaux.

Z

Zettaoctet : Unité de mesure de stockage numérique équivalant à un trillion de gigaoctets, utilisée pour quantifier les volumes de données traitées.

ANNEXE 1 : IMPACT DE LA FRAUDE DOCUMENTAIRE PAR SECTEUR :

Secteur	Méthode et commentaires	Pertes annuelles estimées
Santé	<p>Fraudes liées aux fausses cartes vitales et ordonnances.</p> <p>Si les estimations de cartes surnuméraires sont complexes et changeantes, la commission des affaires sociales de l'Assemblée nationale déclarait en novembre 2020 que l'écart entre le nombre de cartes vitales et le nombre de bénéficiaires potentiels pouvait être estimé à environ 1,8 million.</p>	2,7 milliards € estimés (60% des 4,5 milliards € chiffrés par la cour des comptes en 2024)
Assurantiel	<p>Faux justificatifs :</p> <p>Les types de fraudes affichant les taux de réussite les plus élevés sont les fraudes à l'assurance et à la garantie, toutes deux réussissant dans 80% des cas.</p>	2,5 milliards d'euros de pertes annuelles.
Bancaire	<p>Parmi les fraudes bancaires courantes, on distingue deux mobiles différents :</p> <ul style="list-style-type: none">• Les fraudes à la souscription ;• Les fraudes au financement, et notamment toutes les problématiques liées à la LCB-FT (Lutte contre le blanchiment d'argent et le financement du terrorisme). <p>La Banque de France (2023) rapporte une augmentation de 37 % des fraudes liées aux moyens de paiement, entraînant des coûts élevés pour sécuriser davantage les processus.</p>	<p>En France, le montant de la fraude bancaire en 2023 s'élevait à plus de 1 milliard d'euros.</p> <p>La fraude bancaire s'élève à 4 200 euros en moyenne par personne ayant fraudé.</p>

Secteur	Méthode et commentaires	Pertes annuelles estimées
Immobilier	<ul style="list-style-type: none"> • Dans le secteur de l'immobilier, la fraude à la location est la plus répandue. Selon l'agence blue, 67 % des locataires falsifient leur dossier de location pour se loger. • Les vendeurs malhonnêtes dissimulent des problèmes structurels ou des vices cachés. De manière très simple, ils modifient un titre de propriété, un contrat de vente ou un Diagnostic de Performance Energétique (DPE). • Selon l'Agence de contrôle prudentiel et de résolution (ACPR) de la Banque de France (2024), le préjudice lié aux fraudes aux crédits immobiliers dépasse maintenant le milliard d'euros en France. 	Plus de 1 milliard d'euros
Fiscalité	<p>Falsification de documents pour évasion fiscale</p> <ul style="list-style-type: none"> • La sous-déclaration de revenus locatifs. Les propriétaires omettent volontairement de déclarer leurs revenus locatifs ; • La sous-évaluation des biens immobiliers. Les propriétaires sous-évaluent la valeur des biens immobiliers afin de réduire ces taxes foncières ou l'IFI. Le rapport de la cour des comptes sur l'IFI de janvier 2024 a constaté que l'actualisation annuelle des valeurs déclarées par les redevables de l'IFI ont progressé moins fortement que les prix de l'immobilier¹⁹ ; • La non-déclaration de gains en capital. 	Plus de 60 milliards d'euros

19. Cour des comptes – Rapport L'impôt sur la fortune immobilière

ANNEXE 2 : RÉCAPITULATIF DES DONNÉES STATISTIQUES DU RAPPORT

Statistique	Valeur	Source	Année	Secteur concerné
Fraude documentaire en France	65 milliards € (2,5% du PIB)	Estimation de l'Observatoire Tessi	2025	Global
Augmentation des fraudes numériques (2023-2024)	244%	Fraud Identity report	2025	Global
Entreprises françaises ciblées par la fraude documentaire	69%	Étude Allianz DFCCG	2022	Global
Grandes entreprises (CA > 100M€) ciblées	91%	Étude Allianz DFCCG	2022	Global
Français admettant avoir utilisé des faux documents	10,8%	Étude Selvitys pour Finovox	2024	Global
Taux de réussite des fraudes documentaires	73%	Étude Selvitys pour Finovox	2024	Global
Fraudes numériques (vs physiques)	57%	2025 Identity Fraud Report	2024	Global
Français ayant falsifié des documents pour compte bancaire/crédit	17%	Étude IN BANQUE sur « Les Français et leur banque », réalisée en partenariat avec Capgemini Invent et Tessi (2024)	2024	Bancaire
Taux de fraudeurs chez les moins de 35 ans	>20%	Étude IN BANQUE sur « Les Français et leur banque », réalisée en partenariat avec Capgemini Invent et Tessi (2024)	2024	Bancaire
Fraudes liées à l'usurpation d'identité en Europe	50%	ONDRP	2022	Identité
Victimes d'usurpation d'identité en France	210 000	Ministère de l'Intérieur	2022	Identité
Documents frauduleux aux frontières UE liés à l'usurpation d'identité	68%	Europol	2022	Identité
Dossiers bancaires contenant des justificatifs falsifiés	10-15%	LexisNexis	2021	Bancaire

Statistique	Valeur	Source	Année	Secteur concerné
Tentatives de fraude bancaire impliquant des documents falsifiés	15%	LexisNexis	2021	Bancaire
Pertes liées aux fraudes aux cartes bancaires en France	251 millions d'euros	Observatoire de la Sécurité des Moyens de Paiement	2023	Bancaire
Assurés français ayant falsifié au moins un document	20%	Étude « Innovation Assurance » (Tessi)	2025	Assurance
Fraude sociale en France	20%	Étude « Innovation Assurance » (Tessi)	2025	Assurance
Entreprises ayant subi une fraude à la facturation	13 milliards € / an	Haut conseil du financement de la protection sociale (HCFiPS)	2024	Social
Employeurs ayant détecté une fraude sur les diplômes	46%	PwC	2022	Secteur privé
Faux diplômes circulant en France chaque année	50%	Credence et Prospects	2021	Education
Pertes liées à la fraude bancaire en France	20 000	CNCP	2024	Education
Coût moyen par fraude bancaire réussie	Plus de 1 milliard d'euros €	Observatoire de la Sécurité des Moyens de Paiement	2023	Bancaire
Augmentation des fraudes liées aux moyens de paiement	4 200 €	Selvitys pour Finvox	2023	Bancaire
Pertes annuelles dans le secteur de l'assurance	2,5 milliards €	Lutte contre la Fraude à l'Assurance (ALFA)	–	Assurances
Taux de réussite des fraudes à l'assurance et à la garantie	37%	Banque de France	2023	Bancaire
Fraudes bancaires générées par l'IA	2,5 milliards €	Lutte contre la Fraude à l'Assurance (ALFA)	–	Assurances
Falsification via logiciel de retouche d'image	42,5%	Rapport Signicat	2024	Bancaire

Statistique	Valeur	Source	Année	Secteur concerné
Falsification via IA générative	29%	Rapport Signicat	2024	Bancaire
Falsification via site internet spécialisé	34%	Étude « Innovation Assurance » menée par Next Content en partenariat avec Tessi et Vector8 (février 2025)	2025	Technologie
Estimation de la fraude documentaire dans la fraude fiscale	32%	Étude « Innovation Assurance » menée par Next Content en partenariat avec Tessi et Vector8 (février 2025)	2025	Technologie
Organisations prévoyant d'intégrer des systèmes biométriques d'ici 2025	30%	Étude « Innovation Assurance » menée par Next Content en partenariat avec Tessi et Vector8 (février 2025)	2025	Technologie
Institutions financières européennes expérimentant la blockchain	60 milliards €	Observatoire Tessi	2024	Fiscal
Dossiers de location en Île-de-France comportant un élément falsifié	70%	Gartner	2019	Gartner
Locataires falsifiant leur dossier de location	35%	IDC	2023	Technologie
Dossiers de location en Île-de-France comportant un élément falsifié	23%	Imodirect	Février 2024	Immobilier
Locataires falsifiant leur dossier de location	67%	Agence blue	2020	Immobilier

Annexe 2 : Récapitulatif des données statistiques du rapport

L'OBSERVATOIRE TESSI DE LA FRAUDE DOCUMENTAIRE

Premier centre d'expertise dédié en France, l'Observatoire TESSI de la fraude documentaire répond à un besoin stratégique d'anticipation face à ce phénomène en constante évolution.

Face à la fraude documentaire qui représente une menace systémique pour l'économie française, notre mission s'articule autour de trois axes complémentaires :

- La production d'analyses de référence via un rapport annuel cartographiant les fraudes par secteur d'activité ;
- Une veille continue des évolutions technologiques et réglementaires ;
- L'animation d'un réseau d'experts pour partager les bonnes pratiques et solutions.

L'Observatoire réunit des experts pluridisciplinaires (cybersécurité, analyse documentaire, IA, juridique) maîtrisant les technologies d'intelligence artificielle et de détection des fraudes sophistiquées. Cette expertise est enrichie par des partenariats stratégiques avec des institutions académiques et des organismes spécialisés, positionnant l'Observatoire comme point de référence national en matière d'analyse et de prévention de la fraude documentaire.



tessi

**L'OBSERVATOIRE TESSI
DE LA FRAUDE DOCUMENTAIRE
RAPPORT INITIAL 2025**

Tessi

14 rue des arts et métiers
38000 Grenoble
Tél. +33 (0)4 76 70 59 10

www.tessi.eu